



Privacy Impact Assessment (PIA)

Waiver Review System (WRS)

Version 03.06.01.01

Last Updated: December 2, 2013

1. Contact Information

Department of State Privacy Coordinator
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** December 2,, 2013
- b. **Name of system:** Waiver Review System
- c. **System acronym:** WRS
- d. **IT Asset Baseline (ITAB) number:** # 415
- e. **System description (Briefly describe scope, purpose, and major functions):**

The Waiver Review System (WRS) is designed to support the Bureau of Consular Affairs, Visa Office, Legal Waiver Division (CA/VO/L/W). WRS is an information system used to track the application and adjudication process of exchange visitors, with J Visas seeking to waive the two-year foreign residency requirement 212(e) of the Immigration and Nationality Act. WRS consists of two additional subsystems: the J Visa Waiver Online (JWOL) and Internet Status Check System (ISCS).

The JWOL web site allows exchange visitors desiring a waiver of 212(e) to reserve a case number and begin the paperwork for their request to the Department of State Waiver Review Division for a waiver recommendation. The exchange visitor or representative controls the data entry to ensure an error-free submission. The JWOL creates a bar-coded, hard copy only form that the applicant mails in for processing by the Waiver Review Division. When the form is initially processed, the applicant is provided with a Waiver Review Case Number via return mail. Any applicant (exchange visitor) who has a Waiver Review Case Number can use the ISCS website to check the status of their case. The ISCS provides two text fields offering the status of the two most recent actions on the case and the date the information was retrieved. No personally identifiable information (PII) is collected, supplied, or retained by the ISCS.

- f. **Reason for performing PIA:**

☐ New system

- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

g. Explanation of modification (if applicable): N/A

h. Date of previous PIA (if applicable): September 8, 2009

3. Characterization of the Information

The WRS system:

- ☐ Does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ Does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

WRS primarily collects data on foreign nationals as part of the J visa waiver application process. As such, the information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

Because J visa waiver applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the Privacy Act. However, a WRS record may include PII about persons representing the J visa waiver applicant who are US citizens or legal permanent residents. In addition, the State Department protects and handles PII of non-U.S. persons identically to that of U.S. persons.

The following PII is collected and maintained by WRS: contact information for the applicant, their attorney, representative, and/or organization, specifically their name, address and phone number, fax number, and email address. In addition, the system collects and maintains applicant birthdates and individual ID numbers. The source of information is the exchange visitor or representative (e.g., attorney) completing the form on the visitors behalf.

b. How is the information collected?

The information is collected from applicants who use the J Visa Waiver Recommendation Application on the JWOL web site.

c. Why is the information collected and maintained?

To allow a J-1 exchange visitor ("EV") to request a waiver of the two-year home country requirement.

d. How will the information be checked for accuracy?

Accuracy of the information provided on the forms is the responsibility of the applicant. Applicant information is also vetted in the normal course of waiver request processing.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)
- Mutual Educational and Cultural Exchange Act of 1961

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

With the collection of visa records, WRS has moderate confidentiality and moderate data integrity risks. The primary risk is misuse by Department employees and contractors. Misuse of PII could result in delays in processing applications. Misuse may also result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress for applicants whose PII is compromised. In addition to administrative burdens, data compromises may escalate to financial loss; loss of public reputation and public confidence; and civil liability for the Department of State.

The Department of State seeks to address these risks by minimizing the collection and transmission of PII to the smallest amount required to perform the function of Waiver Review. Collecting this type of sensitive information results in a greater risk but this risk is mitigated by numerous management, operational, and technical security controls in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling,

configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports.

In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized users with a need to know are granted access to WRS.

Based on these mitigating controls, there is an acceptable level of risk associated with WRS processing of PII data.

4. Uses of the Information

a. Describe all uses of the information.

The information managed by WRS is used solely by waiver officers for the purpose of initiating, handling, and tracking of J Visas waiver requests. What types of methods are used to analyze the data? What new information may be produced?

As part of the waiver recommendation process, WRS interfaces with the Consular Lookout and Support System (CLASS) to perform name checks, and with the Consular Consolidated Database (CCD) to associate waiver information with visa information. The result of the name check request (hit or no hit) is used in making a waiver recommendation that can be one of the following:

- Favorable
- Not Favorable
- Subject
- Not Subject
- Inactive
- Withdrawn
- Ineligible

b. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

WRS does not use commercial information, publicly available, or information from other Federal agency databases.

c. Are contractors involved in the uses of the PII?

WRS is a government owned system. Government personnel are primary users of WRS. However, both government personnel and contractors are involved with

the design, administration, and maintenance of the system. CA contractors may be given access to WRS in a user or administrator role giving them access to PII if needed to perform their assigned duties. This includes cases where PII is captured in audit logs, transaction logs, or other system logs.

All users are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

d. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

There is an acceptable level of risk associated with WRS processing of PII data based on the mitigating controls which are in place as described in this section including restricting access to the system, providing guidance to users as to acceptable use of the system, and restricting use of system functions to those defined by business requirements.

The Department of State's Consular Consolidated Database is used to maintain user accounts and user roles for the WRS application. Mandatory annual security and privacy training is required for all authorized users including security training and regular refreshment training.

Guidance with regard to acceptable use of government systems and privacy information in particular is provided in the following ways. User access to information is restricted according to job responsibilities and requires managerial level approval. Access control lists detail categories of information and reports that are to be restricted. Management determines the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

Contractors who support WRS are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors who require access to, and install or maintain WRS hardware and software deployed in support of the Department must have a level "Secret" security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) are allowed to access the server rooms housing the WRS.

All attempts to modify or delete WRS records will create a record of the action in the audit trail and/or system logs. Additionally, the system is configured in accordance with the principle of least functionality to ensure that only essential capabilities are enabled.

5. Retention

a. How long is information retained?

When a case is open and active, the data is retained and accessible through WRS to facilitate case adjudication. A WRS records is retained for 11 years following the final determination on the waiver request and then the record is destroyed in accordance with US Department of State Records Schedule Section A-14-001-26.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater the risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of information aging. Accuracy of the data is dependent on the individuals providing accurate self-identifying information. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of WRS throughout the lifetime of the data.

Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with published Department of State Record Disposition Schedule, approved by the National Archives and Records Administration.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The only internal organization that has access to WRS data is the Bureau of Consular Affairs (CA). Specifically, WRS information is shared with Department of State Adjudicators who are the individuals responsible for processing a waiver application; typically, the Waiver Review Officer. In addition, WRS interfaces with the Consular Lookout and Support System (CLASS) to perform name

checks, and with the Consular Consolidated Database (CCD) to associate waiver information with visa information.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files is protected by passwords, and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing PII internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of PII by personnel can result from social engineering, phishing, abuse of elevated privileges or a general lack of training.

Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

To combat the misuse of information, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure, including, but not limited to, annual security training, separation of duties, personnel screening, and auditing.

These risk factors are mitigated through the use of Technical, Management, and Operational security controls in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). WRS application data is protected by multiple layers of system security. The defense-in-depth system security includes State Department intranet security, WRS application security, Department of State site physical security and management security. These controls include annual security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling,

configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Waiver recommendations are forwarded to the Department of Homeland Security (DHS) Citizenship and Immigration Service (CIS) for a final decision. While the Waiver Review Division is responsible for issuing recommendations, DHS has the final authority to approve or deny waiver requests.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

WRS does not directly connect to any systems outside of the State Department. WRS information is replicated to CCD which in turn communicates with external agencies. The CCD system and its communications with external agencies are external to the WRS boundary. The CCD uses secure transmission methods permitted by Department policy for the handling and transmission of Sensitive But Unclassified (SBU) information. Security officers determine the access level depending on job function and level of clearance. More information about data sharing through CCD can be found within the CCD PIA.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

WRS information is replicated to CCD which in turn communicates with external agencies. The CCD system and its communications with external agencies are external to the WRS boundary. More information about data sharing through CCD can be found within the CCD PIA.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.
Visa Records State -39

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

The information provided by the J visa waiver applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The J Visa Waiver Recommendation application form provides a statement that the Department of State assures that it will not:

- Obtain personal identifying information about you, unless you choose to provide such information
- Share any information it receives with any outside parties, except for authorized law enforcement investigations, or as otherwise required by law.

The public facing interface that applicants initially use to reserve a case number does have the standard State Department warning banner stating that WRS is a government system and restrictions on its use. Also, notice is provided in the System of Records Notice Visa Records, State-39.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes, information is given voluntarily by the applicants or their representatives.

Individuals who voluntarily apply for a waiver must supply all the requested information. If they decline to provide part or all the information required, their application for a waiver may be denied.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. Applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is given to individuals as described in Section 8(a) above. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

The information in WRS is considered a visa record subject to confidentiality requirements under INA 222(f).

If individuals believe there is incorrect information regarding the record of their waiver cases, they are instructed to contact VO Public Inquiries at (202) 663-1225, and are given the opportunity to submit amended information.

PII of U.S. citizens and legal permanent residents is protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correct their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR Part 171 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record.

Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

To the extent information in WRS may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is sufficiently mitigated by WRS.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to WRS is limited to authorized Department of State users that have a justified need for the information in order to perform official duties. To access the system, users must be an authorized user of the Department of State unclassified network. Access to WRS requires a unique user account assigned by a Certifying Authority. Each authorized user must sign a user access

agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Management determines the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. The Department of State's Consular Consolidated Database (CCD) application is used to maintain user accounts and user roles for the WRS application. Mandatory annual security and privacy training is required for all authorized users.

Internet based users of Internet Status Check System (ISCS) and J Visa Waiver Online (JWOL) only have access to these systems for the purpose of completing a J Visa Waiver Recommendation Application or checking the status of their application once their application has been assigned a case number. These users are presented with a Computer Fraud and Abuse Act Notice and Privacy Act Notice that they must take explicit action to accept prior to using these systems. These notices outline the expected use of these systems and how they are subject to monitoring.

b. What privacy orientation or training for the system is provided authorized users?

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

All contractors involved with the design, development, and maintenance have Privacy Act clauses in their contracts and all other regulatory measures have been addressed. They are informed of the established rules of conduct and undergo training on handling information under the Privacy Act of 1974, as amended.

Internet based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

- c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.**

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.). Based on the WRS safeguards provided, there is an acceptable level of residual risk regarding unauthorized access to PII data.

11. Technologies

- a. What technologies are used in the system that involves privacy risk?**

WRS does not employ any technology known to specifically elevate privacy risk.

- b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.**

Since WRS does not use any technology known to specifically elevate privacy risk, the current system safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

- a. What is the security certification and accreditation (C&A) status of the system?**

Department of State operates WRS, and subsystems ISCS and JWOL, in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and has implemented those controls. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial reauthorization of this system, a full assessment of WRS and subsystems ISCS and JWOL was completed and a three year Authority to operate was granted on November 30, 2013.